MEMORANDUM

TO: Mary Ann Borgeson, Chair, Douglas County Commissioner
Clare Duda, Vice-Chair, Douglas County Commissioner
Mike Boyle, Douglas County commissioner
Marc Kraft, Douglas County commissioner
PJ Morgan, Douglas County Commissioner
Chris Rodgers, Douglas County Commissioner
Pam Tusa, Douglas County Commissioner
Thomas Cavanaugh, Douglas County Clerk/Comptroller
John Ewing, Douglas County Treasurer

CC: T. Paul Tomoser, Audit Committee Chair
Jack Armitage
Ron Bucher
Joni J. Davis
Kathleen Kelley, Chief Administrative Officer
Joe Lorenz, Director of Budget and Finance
Kathleen Hall, Chief Deputy Douglas County Clerk/Comptroller
Jerry Prazan, Finance Administrator Douglas County Clerk/Comptroller
Patrick Bloomingdale, Deputy County Administrator
Tim Cavanaugh, Chief Deputy Treasurer
Patricia Carter, Senior Director of Accounting/Auditing Treasurer
Fred Weber

FROM: Mike Dwornicki, Internal Audit Director

DATE: July 15, 2011

SUBJECT: Oracle User Access

Background

As part of the fiscal year audit plan, Douglas County Internal Audit performs internal control testing for the Douglas County external audit firm, Hayes and Associates, LLC. The external auditor uses the test data provided by Internal Audit to formulate a professional opinion about the County's year-end financial statements. Below are the details related to tests of the controls for Oracle user access.

Objectives

The objectives of the audit were to determine that:

- Employee Oracle user access is authorized and approved by appropriate personnel.

- There are appropriate controls in place to ensure that Oracle users' access rights are restricted to the functions that are essential to their job description and that the access does not create a segregation of duty conflict.

- Oracle user access for all employees is periodically assessed for propriety.

Scope and Methodology

The audit included a review of thirty randomly chosen Oracle access requests from July 1, 2010 through April 20, 2011. The sample was chosen using the current and prior active Oracle user listings. The review verified that the access requested was approved by the appropriate managers and that the access granted was the access authorized. Generation of appropriate notices and removal of access was also verified for Oracle users upon termination.

The periodic assessment of user access was reviewed to determine how user access was evaluated. Additionally, the duties of all Douglas County employees with the ability to update data within Oracle were analyzed to determine if there were any segregation of duty conflicts.

Findings

Conflicts of Duties and Oracle User Assessment

Criteria: Access to accounting and financial records should only be provided in accordance with management's approval which provides for adequate segregation of duties. Those duties should be periodically assessed and include an evaluation to ensure that current system access provides for adequate segregation of duties and that employees have only the access needed to do their jobs.

Condition: Analysis of Oracle user access revealed exceptions related to employees with incompatible duties and terminations. The exceptions noted follow:

- Four employees had Oracle access that provided the ability to apply receipts to customer invoices and had access to the cash receipts. One of the employees also had the ability to create credit memos.
- One employee that transferred departments had access that was not requested.
  - Note: The unrequested access has been removed.

- A comparison of listings of active Oracle users to the active employees revealed that there were eight former employees that had active Oracle log-ins.

Effect: The effects of the above conditions are outlined below:

- The employees who had access to apply cash receipts and access to the cash receipts had the opportunity to convert cash receipts to personal use and possibly avoid detection.

- The access of the transferred employee provided more access than was needed to do their job.

- Terminated employees having active log-ins provided the former employees an opportunity to possibly access information that could cause real or reputational harm to Douglas County.

Cause: Mandating County-wide standards for receiving and applying cash receipts may have prevented cash receipt conflicts from occurring. A more comprehensive user access assessment may have brought the conflicts of duties to light. The person assessing Oracle user access had knowledge of the duties within their own department, but not outside of that department. Without this knowledge a complete and accurate assessment of segregation of duties could not be conducted. Lastly, the active user listing was not used to determine that only active employees had Oracle user access.

Recommendation: To address the conflict of duty issues consider the following:

- The Treasurer's Department should Draft County-wide standards outlining the appropriate procedures to follow when receiving and applying cash receipts.

- Ensure that the employees with the ability to apply cash do not have access to the cash receipts or provide mitigating controls to ensure all receipts in their possession is deposited intact.

Improve the periodic user assessment by incorporating the following additional analysis into the evaluation:

- Confirm that the duties of persons with the ability to update information within Oracle do not conflict with their Oracle user access.

- Use a current employee listing to determine that only active employees have access to Oracle.

Management Response to 1st and 2nd bullet: The Treasurer's Office is researching policies and procedures to appropriately address the cash receipt issues identified.

Management Response to 3rd and 4th bullet: Management does review Oracle user access reports to assure appropriate segregation of duties and termination of access for terminated employees, but agrees this process can be improved upon. The County's Internal Auditor has offered to share a programmatic method of performing this task that can help effect this improvement.

Functional Lead Access

Criteria: System Administrator access should be provided to as few persons as possible and only provided to those needing it to perform their job functions.

Condition: It was noted that the Oracle Functional Leads have extensive Oracle access including System Administrator log-on capability. This capability can be used to gain access to all applications and data and also provides the ability to set security parameters. The Chief Deputy Douglas County Clerk indirectly monitors the Leads' activity by reviewing master data change alerts, payments, and budget activity. An examination of the master data alerts indicated that there was no alert generated when employee direct deposit bank account information was changed.

Effect: The Leads’ level of access provided the ability to make unauthorized changes within Oracle and possibly avoid detection. Due to the nature of the Leads’ access, unauthorized activity may not be detected by the current review (e.g., changes made to alert reports). Without an alert for bank account changes, unauthorized modifications to account information may not be detected. Unauthorized changes could lead to the conversion of County assets to personal use possibly without detection.

Cause: The Leads’ have Oracle access that would not normally be provided for their job functions. System Administrator access was provided to the Leads to handle operational problems for users (e.g., queries or reports that are caught in loops) that is normally handled by IT Operations.

Recommendation: Management should consider the following to mitigate issues related to the Functional Leads’ system access:

- Determine if Oracle System Administrator duties can be split to remove user access change capability. Alternatively, management may want to transfer all duties performed by the Leads that require System Administrator access to IT Operations personnel.
    - Note: A user request was created to develop new responsibilities for the Functional Leads and their subsequent removal from System Administrator access.
- Create a new Oracle alert report for changes to direct deposit account information.
    - Note: A user request was created to develop a new Oracle alert for changes to direct deposit account information.

Management Response: The Clerk/Comptroller’s office has requested DOT.Comm investigate the possibility of customizing the Sys Admin responsibility in order to remove user access change capability. The Clerk/Comptroller’s office has requested DOT.Comm develop an automated Oracle alert to notify of any changes to direct deposit account information. Attached please find a listing of the items included in the Sys Admin responsibility that are used on a regular basis to assist our staff in performing the business processes of this office.

Audit Standards

Internal Audit conducted this audit in accordance with generally accepted government auditing standards. Those standards require that the audit is planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Internal Audit believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objectives.

****

Internal Audit has reviewed this information with the Chief Deputy Douglas County Clerk, the Treasurer's Senior Director of Accounting/Auditing, and the DOT.Comm Information Services Manager. Internal Audit appreciates the excellent cooperation provided by management and staff. Please provide your responses within two weeks of receiving this report. If you have any questions or wish to discuss the information presented in this report, please contact Mike Dwornicki at (402) 444-4327.

Attachment

Concurrent

Requests - Running Requests

Set - Setting up and running request sets

Conflicts Domains

Concurrent : Manager

Administer – Trouble shooting

Define - Trouble shooting

WorkShifts

Rule

Concurrent : Program

Define   - Trouble shooting, modifying and creating new ones

Executable - Trouble shooting, modifying and creating new ones

Types - Trouble shooting, modifying and creating new ones

Profile

System – Trouble shooting and setups

Personal – Trouble shooting and setups

Application

Register - Trouble shooting

Function - Trouble shooting

Menu - Trouble shooting

Administer Folders - Trouble shooting

Currency

Network Test - Trouble shooting

Application : Validation

Set - Trouble shooting and setups

Values – Trouble shooting and setups

Application : Flexfield : Key

Segments – Trouble shooting and setups

Aliases – Trouble shooting and setups

CrossValidation – Trouble shooting and setups

Groups – Trouble shooting and setups

Values – Trouble shooting and setups

Accounts – Trouble shooting and setups

Application : Flexfield : Descriptive

Segments – Trouble shooting and setups

Values – Trouble shooting and setups

Application : Document

Define

Categories

Assign

Repositories

Install

Nodes – Trouble shooting and setups

Languages – Trouble shooting and setups

Natural Languages

Viewer Options – Trouble shooting and setups

Territories

Install : Printer

Register – Trouble shooting and setups

Types – Trouble shooting and setups

Style – Trouble shooting and setups

Driver – Trouble shooting and setups

Requests

Run – Trouble shooting and setups

View – Trouble shooting and setups

Set – Trouble shooting and setups

Workflow : Administrator Workflow

Home – Trouble shooting and setups

Developer Studio – Trouble shooting and setups

Business Events

Status Monitor – Trouble shooting and setups

Notifications – Trouble shooting and setups

Administration – Trouble shooting and setups

Workflow : Transaction Monitor

Transaction Monitor – Trouble shooting and setups

Workflow : Oracle Applications Manager

Workflow Manager – Trouble shooting and setups

Workflow : Web Services WSDL

Generic XMLGateway WSDL – Trouble shooting and setups

Workflow : Worklist Flexfields Rules

Worklist Flexfields Rules – Trouble shooting and setups

Worklist Flexfields Rules Simulation – Trouble shooting and setups

Security

Web PL/SQL

Security : User

Define - Troubleshooting

Monitor - Troubleshooting

Security : Responsibility

Define - Troubleshooting

Request - Troubleshooting

Security : Responsibility : ValueSet

Define - Troubleshooting

Assign - Troubleshooting

Security : ORACLE

Register

DataGroup

Security : AuditTrail

Install

Groups

Tables

Security : AuditTrail : Audit Trail Reporting

Audit Industry Template

Audit Hierarchy Navigator

Audit Query Navigator

Audit Report

Oracle Applications Manager

Workflow – Trouble shooting

License Manager – Trouble shooting

Diagnostics – Trouble shooting

Service Fulfillment Manager

Patching and Utilities – Trouble shooting

Cloning

Hosts

Purging/Critical Activities – Trouble shooting

System Alerts – Trouble shooting

Logs

Applications Usage

Business Flows

Database Status – Trouble shooting

System Configuration Overview – Trouble shooting

Forms Monitoring – Trouble shooting

Concurrent Managers – Trouble shooting

Concurrent Requests – Trouble shooting

JServ Usage

Dashboard – Trouble shooting

OAM Setup